Journal of Engineering, Project, and Production Management
2026, 16(5), 2025-262

Blockchain Traceability Design for Green Agricultural Products Based on an Improved PBFT Consensus Algorithm

Qiaoling Yan
Director, School of Finance, Zhengzhou College of Finance and Economics, Zhengzhou, 450003, China, E-mail: PPQM6789@163.com

Production Management
Received November 9, 2025; revised January 21, 2026; accepted April 14, 2026
Available online June 17, 2026

Abstract: According to FAO statistics, global economic losses due to a lack of transparency in agricultural product information exceeds 30 billion USD annually. This highlights the need for a credible traceability system. The demand for green agricultural product traceability has increased rapidly, while traditional centralized systems remain vulnerable to tampering and inefficient collaboration. Although blockchain offers decentralization and immutability, the traditional Practical Byzantine Fault Tolerance (PBFT) algorithm faces efficiency and security bottlenecks as the network expands. To overcome these challenges, an improved PBFT-based blockchain traceability model is proposed, featuring hierarchical node management and a multi-indicator dynamic scoring mechanism for adaptive leader selection and malicious node elimination. The model builds a full-lifecycle traceability framework encompassing production, processing, logistics, sales, and consumption. Comparative experiments with PBFT and Linear Randomized Byzantine Fault Tolerance (LRBFT) on a 100-node network showed that the improved model achieved 3600 TPS, reduced confirmation time to 200ms at 10ms latency, and maintained 96 percent availability even with 40 percent Byzantine nodes. The tampering detection rate exceeds 94 percent under high-intensity attacks, and multi-party collaboration efficiency improves significantly. These results demonstrate the system's enhanced performance, robustness, and scalability, indicating its strong potential for practical deployment in green agricultural product traceability systems.

Keywords: Agricultural supply chain, blockchain traceability, distributed systems, food safety, PBFT consensus.

DOI 10.32738/JEPPM-2025-262

1. Introduction

Frequent food safety incidents have heightened public concern about the origins and quality of agricultural products. Green agricultural products are a representative category that emphasizes ecological protection, reduced pesticide use, and sustainable production. These products rely heavily on effective traceability to maintain consumer trust and market credibility (Jannes et al., 2023; Wang et al., 2023). Traditional traceability systems depend on centralized databases prone to tampering, data silos, and limited information sharing, making it difficult to achieve transparent supervision across the product lifecycle (Han and Fang, 2024). Blockchain technology, with its decentralized, immutable, and traceable features, offers an alternative solution and has been increasingly applied in agricultural supply chain management. However, in complex multi-node environments with frequent data exchange, blockchain traceability systems still face performance and security challenges (Lai et al., 2024). The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism offers high consistency and security, but it becomes less efficient as the number of nodes increases. It also lacks dynamic node management, which allows low-performance or malicious nodes to persist (Samanta and Sarkar, 2025). These limitations restrict its suitability for multi-stage, multi-actor traceability applications. Therefore, an improved PBFT-based design is introduced that integrates hierarchical node management and a multi-indicator scoring mechanism to enhance consensus efficiency and reliability. The goal is to create a transparent, trustworthy traceability platform that covers production, processing, logistics, sales, and consumption. This platform will enable comprehensive lifecycle supervision of green agricultural products.

2. Related Works

As an essential consensus mechanism for consortium-blockchain, PBFT offers high throughput and low latency, but its traditional form faces challenges such as high communication overhead, poor scalability, and limited adaptability in heterogeneous Internet of Things (IoT) environments. Researchers have improved PBFT from various angles. Li et al.

(2024) introduced a dynamic adaptive PBFT based on multi-agent systems and reinforcement learning to boost adaptability in the Internet of Things (IoT) scenarios. Somasekhar et al. (2024) applied PBFT to an IPFS-based voting system to ensure tamper-resistant data. Chen and Li (2025) proposed a lightweight asynchronous PBFT variant that reduces bandwidth consumption and increases throughput. Okegbile et al. (2024) added sharding and a reputation mechanism to enhance performance and security. These studies show that optimizing PBFT's communication structure and node management can greatly improve its efficiency and applicability.

Agricultural traceability involves multiple semi-trusted participants such as producers, processors, logistics firms, and regulators, making a high-performance PBFT mechanism particularly suitable. Blockchain traceability applications have expanded rapidly: Guo et al. (2025) enhanced scalability through sharding. Zheng and Zhang (2024) improved stability using a reputation-based consensus. Yadav et al. (2023) identified traceability and decentralized data management as key drivers for blockchain adoption. El Mane et al. (2024) combined blockchain, IoT, and smart contracts to boost workflow automation and data reliability. However, most current studies focus more on blockchain storage or smart contract design rather than on optimizing consensus, which directly impacts real-time performance and scalability.

Previous work improved PBFT efficiency and explored blockchain traceability applications but lacked consensus algorithms tailored specifically for green agricultural product traceability, particularly regarding dynamic node evaluation, leader selection fairness, and end-to-end trust assurance. Consequently, this study proposes an improved PBFT with hierarchical node management and multi-indicator scoring to boost efficiency and security, and develops a comprehensive traceability architecture covering data collection, storage, and multi-party aspects of collaboration.

3. Methods and Materials

3.1. Improving the Design of the PBFT Consensus Algorithm

Green agricultural product traceability involves many nodes, frequent data exchange, and risks of malicious tampering. The PBFT consensus mechanism ensures data consistency and security in multi-node environments (Xinting et al., 2024). However, traditional PBFT incurs rapidly increasing communication costs as the network grows. It also lacks the ability to dynamically manage inefficient or malicious nodes, which limits its applicability to complex traceability scenarios. To improve efficiency and reliability, this study introduces a credit-based hierarchical node management mechanism. This evaluates node performance and credibility using indicators such as reputation, response rate, latency, and energy consumption. Nodes with higher scores become candidates for primary node selection, while low-performing or malicious nodes are excluded from consensus participation. The mechanism supports dynamic node replacement and improves consensus efficiency, as illustrated in Fig. 1.

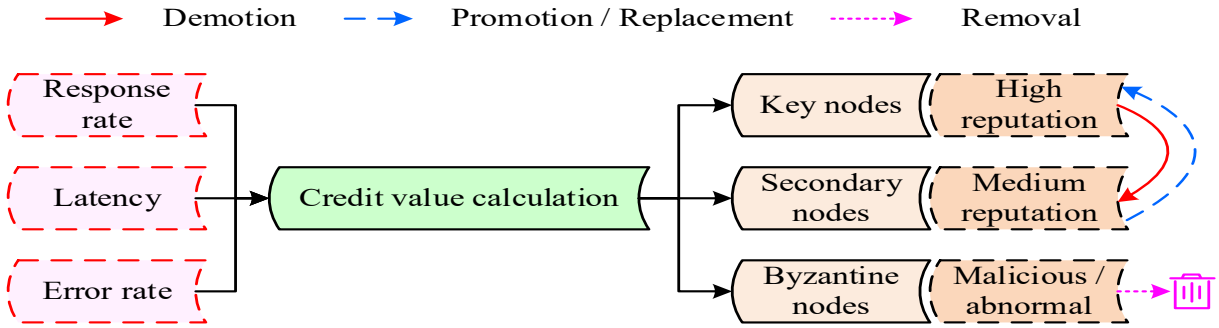

Fig. 1. Node hierarchical management mechanism

As shown in Fig. 1, this mechanism implements hierarchical node management by quantifying node behaviors, calculating credit scores, and automatically classifying nodes. After each consensus round, the system categorizes nodes into high-reputation, secondary, and Byzantine groups based on their credit values. It then dynamically updates their levels, retains the high-reputation nodes, keeps the secondary nodes as backups, and removes the low-reputation nodes. This ensures efficient and trustworthy consensus management. Specifically, the updated formula for a node's credit score in Round $t+1$ is expressed as Eq. (1).

$$R_i^{(t+1)} = \alpha R_i^{(t)} + \beta S_i - \gamma M_i - \delta L_i \tag{1}$$

In Eq. (1), $R_i^{(t+1)}$ represents the credit value of node A in round $t+1$. $R_i^{(t)}$ is the credit value from the previous round. α is the decay coefficient for historical credit, balancing a node's long-term and recent performance. Preliminary parameter sensitivity experiments show that when the value of α is between 0.4 and 0.6, the system achieves optimal levels of availability and stability. S_i denotes the number of normal behaviors exhibited by the node during the current consensus round, such as timely signature returns or valid voting participation. β is the reward coefficient, amplifying the positive contribution of normal behaviors to credit value (Nayal et al., 2023). M_i denotes the number of malicious behaviors exhibited by the node in the current round, such as double-signing, submitting invalid votes, or fabricating information. γ is the penalty coefficient that amplifies the negative impact of malicious behaviors on creditworthiness. L_i represents the number of abnormal behaviors occurring in the current round, including disconnections, timeouts, or prolonged delays. δ is the corresponding penalty coefficient.

During the consensus process, the node hierarchy management system adjusts credit values after each round by rewarding normal behaviors and penalizing malicious or abnormal actions. Based on predefined thresholds, nodes are divided into three categories. Nodes with credit values above the high-reputation threshold are considered primary participants with priority in the consensus. Nodes within the middle range become standby participants, ready to step in when needed (Huang et al., 2025). Nodes with credit values below the minimum threshold or identified as malicious are labeled as Byzantine and removed from the next consensus round. To improve efficiency and security further, a multi-criteria scoring mechanism has been introduced. This mechanism evaluates credibility, response rate, latency, and resource consumption to rank candidate nodes and select the most suitable one as the primary node. It also enables rapid replacement in the event of performance degradation or malicious behavior. The mechanism is shown in Fig. 2.

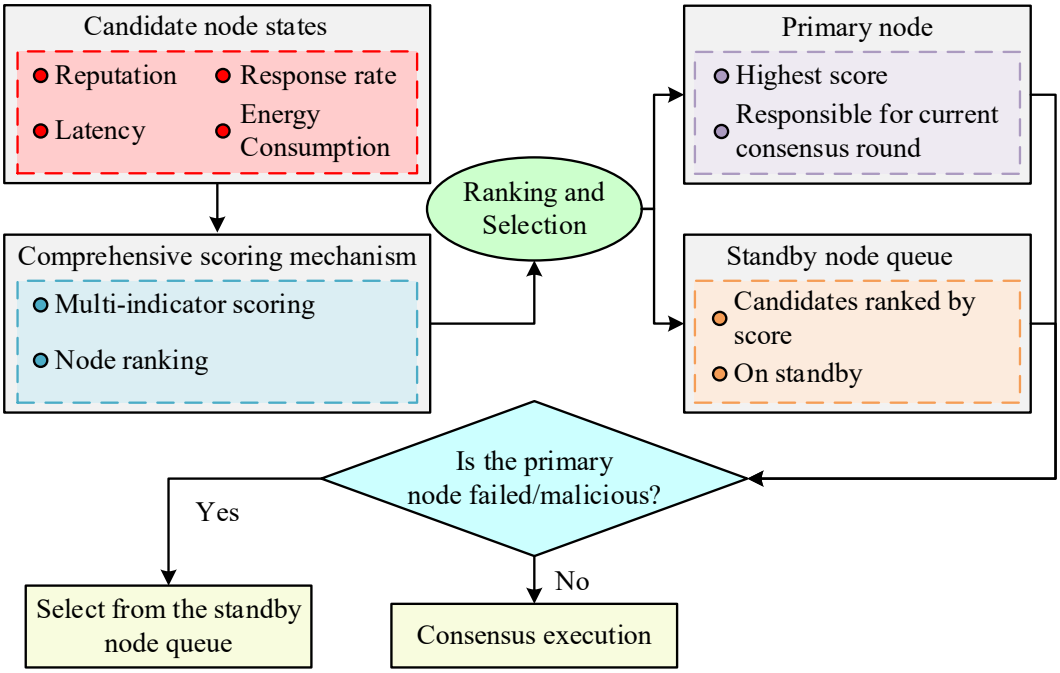

Fig. 2. Multi-index scoring mechanism

Fig. 2 shows that the multi-criteria scoring mechanism evaluates candidate nodes based on four indicators: reputation, response rate, latency, and energy consumption. These indicators are weighted and aggregated to generate a comprehensive score used to rank the nodes. The highest-scoring node is selected as the primary node for the current consensus round, while the others form a standby queue. Should the primary node fail or behave maliciously, the system replaces it with the next-highest-scoring node while demoting the faulty node. This maintains consensus stability and security. The comprehensive score for candidate node i is defined as shown in Eq. (2).

$$S_i = \lambda_1 Q_i + \lambda_2 P_i + \lambda_3 (1 - D_i) - \lambda_4 C_i \tag{2}$$

In Eq. (2), Q_i represents the credibility rating value, derived from the credit mechanism calculation results in the previous section. P_i denotes the response rate, the proportion of messages returned on time. Its value ranges from 0 to 1, with higher values being preferable. D_i indicates the normalized delay value, ranging from 0 to 1, with lower values being preferable. C_i represents the energy consumption or resource utilization value, normalized to a range of 0 to 1. Lower values are preferred, hence it is included with a negative sign.

λ_1, λ_2, λ_3, and λ_4 represent the weight coefficients corresponding to reputation level, response rate, delay, and energy consumption, respectively. The first two indicators are positive, reflecting node trustworthiness and responsiveness, while the latter two are negative, penalizing latency and excessive energy use. The weights are determined through the Analytic Hierarchy Process (AHP) using expert evaluation and consistency verification (CR < 0.1). The final weights of 0.37, 0.31, 0.19, and 0.13 balance performance, responsiveness, and energy efficiency, forming a rational basis for the multi-indicator scoring mechanism.

The proposed node hierarchical management mechanism implements global management, ensuring all nodes entering the consensus set are trustworthy. In contrast, the multi-indicator scoring mechanism performs local optimization, dynamically selecting the optimal primary node from healthy nodes while establishing a backup mechanism. Therefore, combining these two optimization mechanisms, the improved PBFT consensus algorithm process is illustrated in Fig. 3.

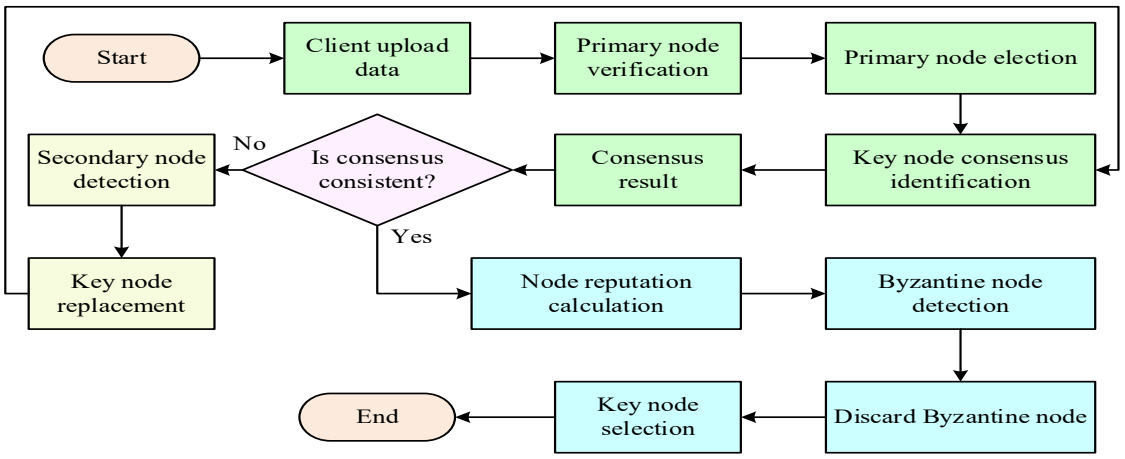

Fig. 3. Process of improving the PBFT consensus algorithm

In Fig. 3, the improved PBFT consensus algorithm evaluates candidate nodes using a multi-criteria scoring system, selects the most suitable primary node, and maintains a standby queue. The primary node initiates proposals and coordinates voting among key nodes. After voting, the system performs a consistency check; valid results trigger the node hierarchical management mechanism, which updates node status based on reputation scores by retaining high-reputation nodes, activating standby nodes when necessary, and removing Byzantine nodes. If the result is invalid, the system replaces the primary node to ensure stable consensus. This closed-loop process enhances communication efficiency, node management, and system robustness, making the algorithm better suited to complex blockchain-based traceability scenarios in green agriculture.

3.2. Blockchain Traceability System Architecture for Green Agricultural Products

While the improved PBFT algorithm offers a reliable foundation for consensus, a consensus mechanism alone cannot meet the complex needs of green agricultural product traceability. Since product circulation involves production, processing, transportation, and sales, the system must support multi-source data collection, distributed storage, and end-to-end traceability (Liu et al., 2023; Mohan et al., 2023). Building on the improved PBFT algorithm, a blockchain-based traceability framework is developed to ensure trustworthy data recording, transparent lifecycle management, and collaborative operation among multiple stakeholders. The overall system architecture is depicted in Fig. 4.

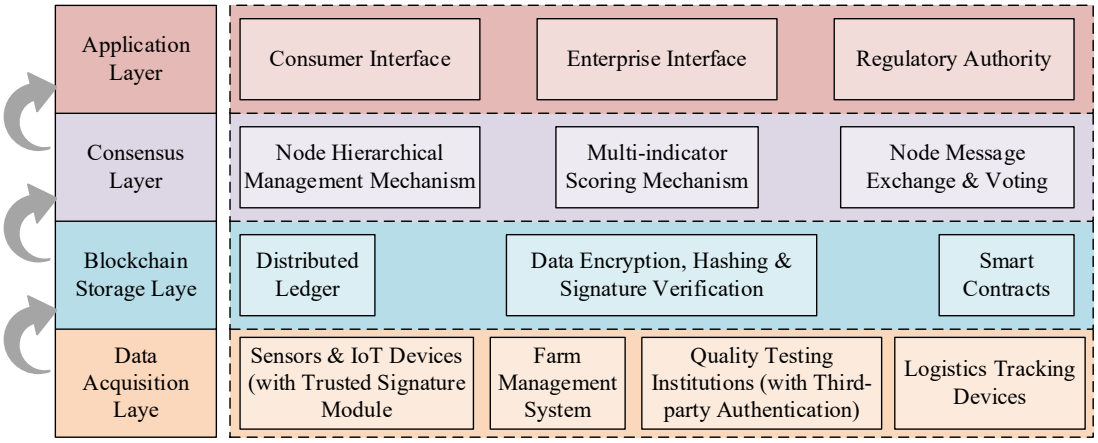

Fig. 4. Schematic diagram of the overall system architecture

As shown in Fig. 4, the system comprises four layers: data acquisition, blockchain storage, consensus, and application. The data acquisition layer enhances traditional IoT access by providing a trusted mechanism for collecting and authenticating data. In this mechanism, devices sign data using private keys, and a third-party Certificate Authority (CA) certification verifies the authenticity of inspection agencies before they upload data. The blockchain storage layer maintains the distributed ledger and performs encryption, hashing, and signature verification to ensure data immutability and secure sharing. The consensus layer uses an enhanced PBFT algorithm with hierarchical node management and multi-indicator scoring to improve efficiency and reliability. The application layer provides unified interfaces for consumers, enterprises, and regulators, enabling transparent traceability and visual management throughout the entire production-to-consumption process. The data acquisition process is described in Eq. (3).

$$D = (d_1, d_2, \ldots, d_n) \tag{3}$$

In Eq. (3), D denotes the complete dataset. d_i represents the traceability data collected at the ith stage. n is the total number of stages covered by the system. Subsequently, these data undergo processing via a hash function prior to being recorded on the blockchain to ensure their uniqueness and tamper-proof nature, as shown in Eq. (4).

$$H(d_i) = \text{SHA-256}(d_i) \tag{4}$$

In Eq. (4), $H(d_i)$ represents the hash value of data d_i. SHA-256$(\cdot)$ is a secure hash function capable of mapping inputs of arbitrary length to a fixed-length 256-bit output, ensuring that even minor alterations to the data result in entirely different hash values. At the consensus layer, the system employs an improved PBFT algorithm to maintain consistency among nodes. If the node set is denoted as $\mathbb{N}$, it must satisfy Eq. (5).

$$|\text{Honest}(\mathbb{N})| \geq \frac{2}{3}|\mathbb{N}| \tag{5}$$

Eq. (5), Honest$(\mathbb{N})$ denotes the number of honest nodes (i.e., normal nodes adhering to the protocol) in the set. $|\mathbb{N}|$ represents the total number of nodes in the network. $\frac{2}{3}|\mathbb{N}|$ signifies the minimum number of honest nodes required to guarantee fault tolerance. This condition ensures the system maintains data consistency even in the presence of a small number of Byzantine nodes. Ultimately, data validated through storage and consensus is transmitted to the application layer for access by consumers, enterprises, and regulatory bodies, enabling transparent and trustworthy traceability services. Fig. 5 illustrates the traceability process for green agricultural products throughout the production-to-consumption lifecycle. It also shows the data chaining and verification pathways.

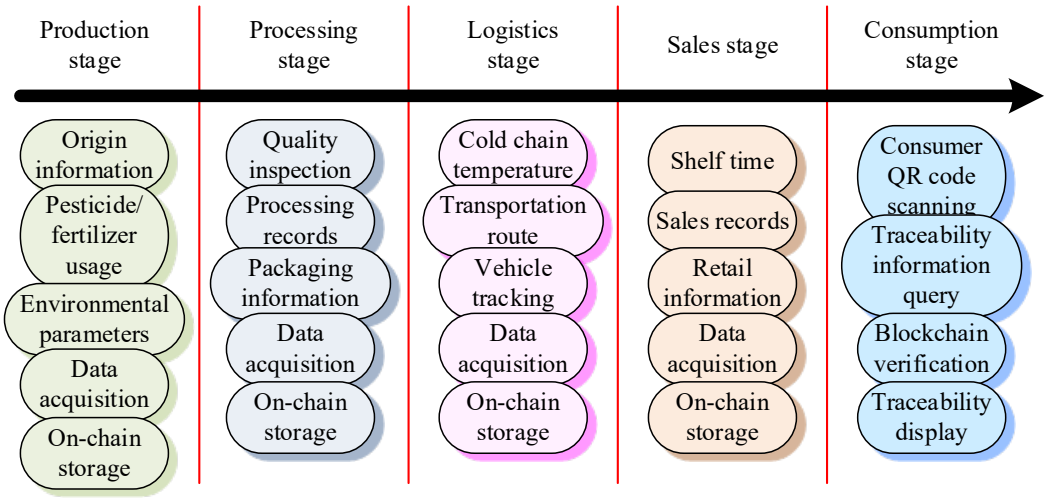

Fig. 5. Traceability process for the entire life cycle of green agricultural products

As shown in Fig. 5, the traceability of green agricultural products covers production, processing, logistics, sales, and consumption, forming a closed loop of data collection, recording, verification, and retrieval. In the production stage, sensors gather data on origin, pesticide and fertilizer use, and environmental parameters, while the improved PBFT algorithm verifies data authenticity through hashing and digital signatures. During processing, quality inspection results and process records are validated and stored on the blockchain. In logistics, real-time transportation routes, cold-chain temperatures, and trajectories are uploaded and verified to prevent tampering. At the sales stage, shelf life and transaction details are confirmed by multiple parties and stored on the distributed ledger, creating a reliable record of product movement. In the consumption phase, users scan a QR code to access lifecycle data and obtain transparent traceability information. By continuously connecting these stages, the system ensures that data is securely collected, verified, stored, and retrieved, establishing a trustworthy traceability chain throughout the lifecycle of green agricultural products.

It is important to note that data collection and uploading across all lifecycle stages are not handled by a single entity. Instead, these activities involve the collaborative participation of multiple stakeholders, including farmers, processing enterprises, logistics companies, testing institutions, regulatory authorities, and consumers. Therefore, the research focuses on building an interactive role model for the blockchain traceability system of green agricultural products, as shown in Fig. 6.

As shown in Fig. 6, the traceability system for green agricultural products creates a trusted data interaction platform supported by an improved PBFT consensus mechanism. Producers, processors, logistics companies, and inspection institutions upload key data from each stage, which are verified for authenticity and integrity before being recorded on the blockchain. Inspection institutions sign test reports using private keys, and a certificate authority validates these signatures to ensure the legal validity and reliability of inspection data. The node hierarchy management mechanism removes low-credibility or malicious nodes, while the multi-indicator scoring system dynamically selects suitable primary nodes to improve consensus efficiency and security. Regulatory authorities perform real-time oversight, and consumers can access complete traceability information by scanning a QR code. This multi-party interaction model guarantees secure collaboration and dependable data sharing throughout the traceability process.

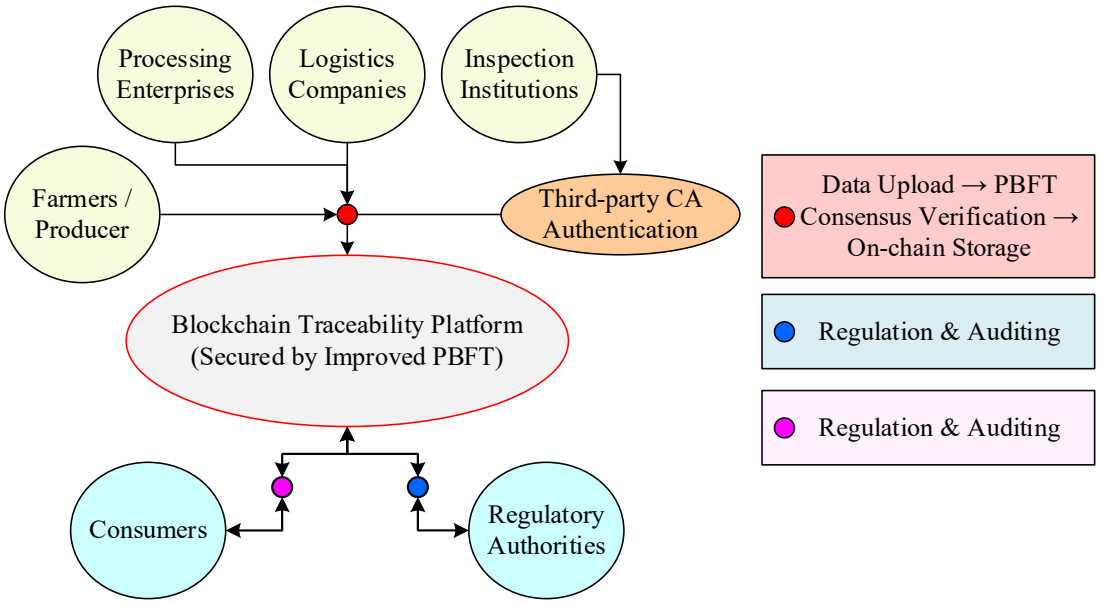

Fig. 6. Interaction among stakeholders in the blockchain traceability system with improved PBFT consensus

3.3. Typical Use Case and Practical Application Process of Green Agricultural Product Traceability

To improve the practical application of the proposed system in real agricultural supply chains, this study creates a representative use case based on actual business workflows. This use case illustrates how data acquisition, stakeholder onboarding, and blockchain consensus interact throughout the process. During the farmer onboarding stage, production entities register through alliance-chain nodes, link sensor devices to product batches, and use device private keys to sign collected data, such as environmental conditions and input usage. The system verifies the signature through a third-party Certificate Authority, after which the data enters the preprocessing module and is submitted to the improved PBFT consensus layer. During the processing and inspection stages, quality inspection agencies authenticate their inspection results using institutional certificates. Before the data is written to the blockchain ledger, the system performs hash verification and consistency checks to ensure the integrity and immutability of the processed records. During the logistics stage, onboard terminals automatically collect and upload cold-chain temperature, location, and other dynamic information to the chain. Meanwhile, the node hierarchical management mechanism filters out abnormal nodes in real time to ensure the reliable synchronization of dynamic data. In the retail and consumer stages, retailers upload shelf information, and consumers can retrieve complete lifecycle records by scanning product QR codes, achieving transparent and trustworthy traceability. This use case demonstrates that the proposed system creates a verifiable data loop throughout the entire production, processing, logistics, and sales chain. This provides a realistic basis for subsequent performance evaluation and pilot deployment.

4. Performance Testing and Practical Analysis of Improved PBFT Algorithms

4.1. Comprehensive Performance Testing of the Improved PBFT Algorithm

All comparative experiments are conducted under a unified hardware and network environment. The platform consists of eight physical servers, each configured with a 16-core, 2.6 GHz CPU, 32 GB of memory, and Gigabit Ethernet. The servers run Ubuntu 22.04. The block size is set to 1 MB, one block is generated for every 100 transactions, and each PBFT round includes the prepare, pre-prepare, and commit stages with a single-round latency of 10ms. A total of 10,000 transactions are executed, and the number of consensus rounds varies with the number of nodes. To evaluate performance in the green agricultural product traceability scenario, the improved PBFT algorithm is compared against traditional PBFT, Raft, and Proof of Stake under identical experimental conditions. Traditional PBFT follows the BFT-SMaRT standard process. Performance is evaluated based on throughput, confirmation time, system availability, and resource utilization under different node scales, network latencies, Byzantine node ratios, and transaction loads. System availability refers to the proportion of time the system can complete valid consensus and service requests, reflecting operational stability. The comparative results are shown in Fig. 7.

Fig. 7(a) shows that the improved PBFT achieves approximately 4,200 Transactions Per Second (TPS) with 10 nodes and approximately 3,600 TPS with 100 nodes. This is higher than the traditional PBFT (3,200-2,000 TPS), Raft (2,800-1,200 TPS), and Proof of Work (PoW) (1,500-800 TPS). In Fig. 7(b), at 10ms latency, the improved PBFT requires around 200ms for confirmation, compared with 300ms for traditional PBFT and Raft, and 800ms for PoW at 500ms, and it records approximately 1800ms. Fig. 7(c) shows that with 40 percent Byzantine nodes, system availability reaches about 96 percent, while traditional PBFT, Raft, and PoW drop to 91 percent, 82 percent, and 78 percent. Fig. 7(d) indicates that at a 500 TPS load, CPU utilization of the improved PBFT is about 20 percent lower than the other algorithms. Validation of hierarchical node management is shown in Fig. 8.

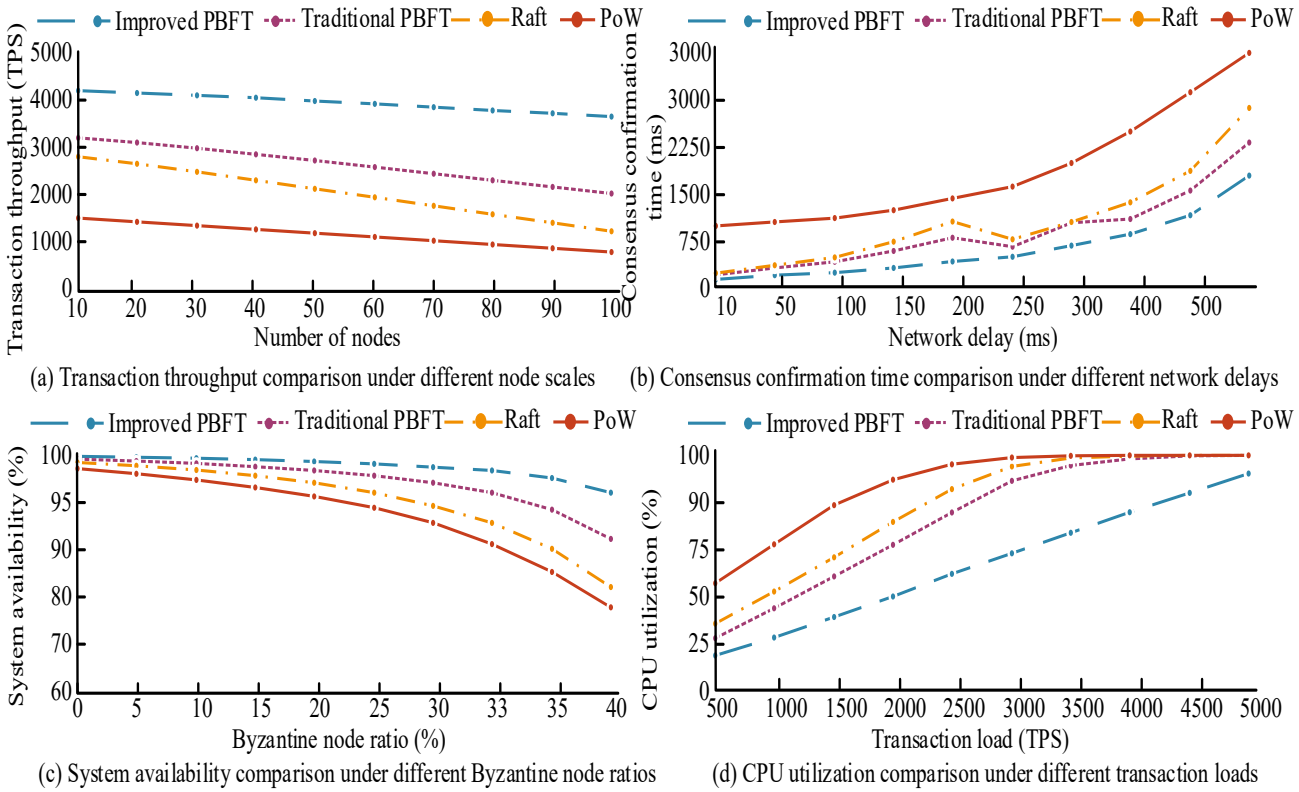

Fig. 7. Performance comparison between improved PBFT algorithm and traditional consensus algorithm

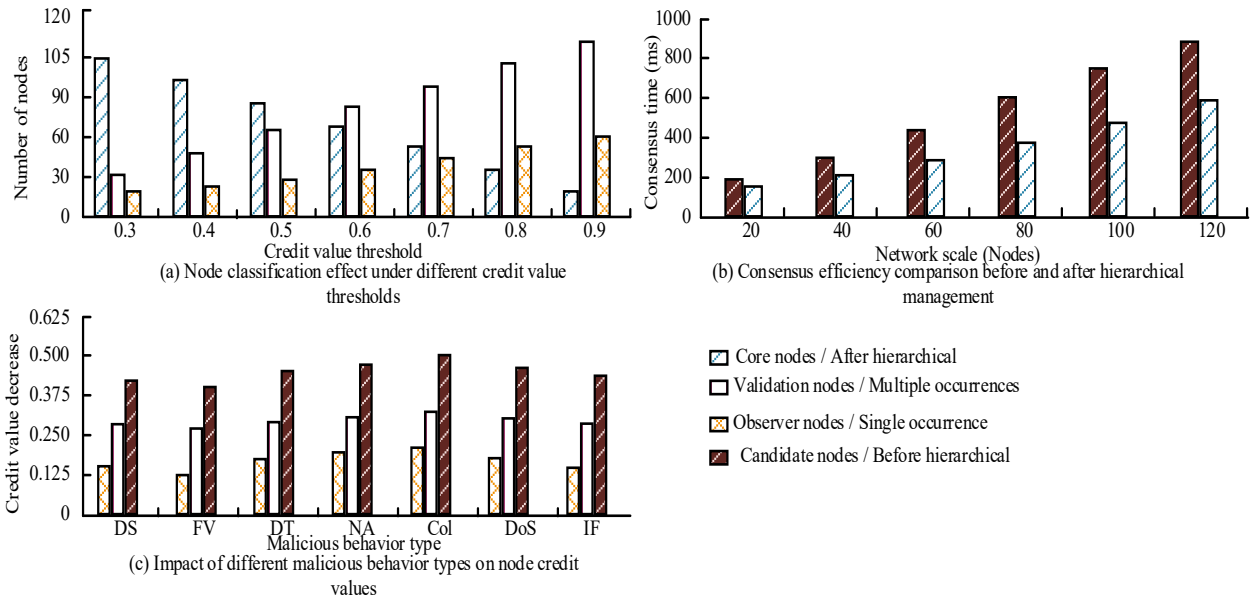

Fig. 8. Verification of the effectiveness of the node hierarchical management mechanism

Fig. 8(a) shows that raising the credit threshold from 60 to 90 increases high-credit nodes from 45 percent to 78 percent, while medium-credit nodes drop from 35 percent to 18 percent and low-credit nodes from 20 percent to 4 percent. Fig. 8(b) indicates that hierarchical management shortens consensus time from 3.2 to 2.1 seconds and increases throughput from 1500 TPS to 2200 TPS. Fig. 8(c) shows that double-spending attacks reduce credibility the most (35 points), followed by sybil attacks (28 points) and malicious voting (15 points). Fig. 8(d) shows stable node replacement performance. The average detection and replacement times are 2.3 and 4.7s, respectively, keeping the total response time within 7 seconds. The correlation analysis of node performance is shown in Fig. 9.

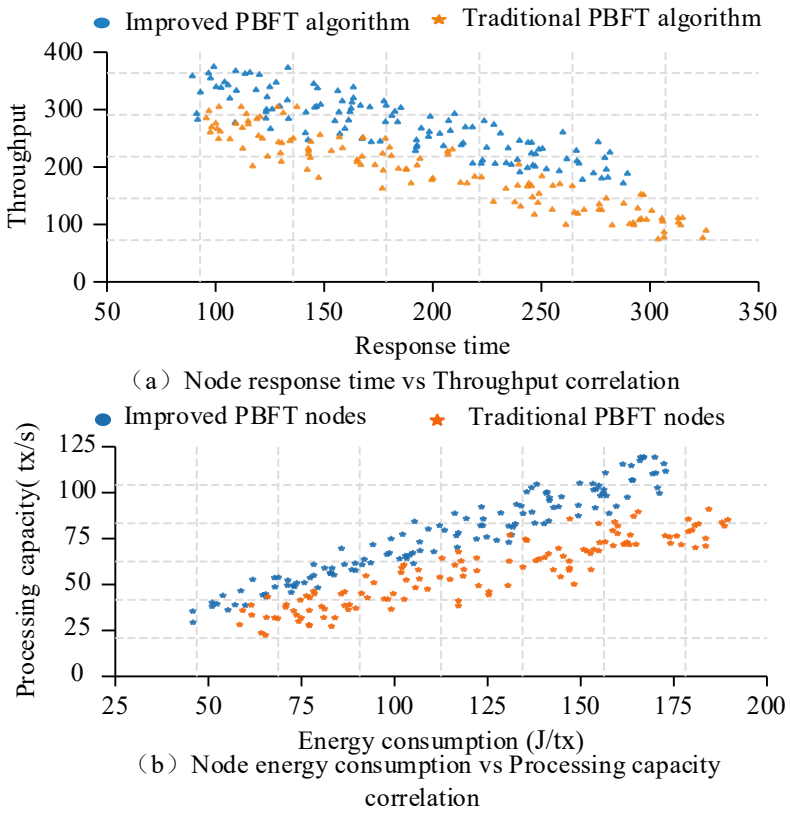

Fig. 9. Analysis of correlation and distribution characteristics of node performance indicators

Fig. 9(a) shows a clear negative correlation between node response time and throughput, with a correlation coefficient of -0.78. When response time increases from 50ms to 350ms, throughput decreases from 350 TPS to 200 TPS. Fig. 9(b) demonstrates that the improved PBFT node reduces energy consumption by 10J/tx compared to traditional methods, significantly outperforming conventional PBFT.

4.2. Applied Analysis of Blockchain Traceability Algorithms for Green Agricultural Products

To evaluate the improved PBFT algorithm's ability to maintain data integrity across the full traceability lifecycle, a monitoring system is established for production, processing, logistics, and sales. The system analyzes changes in integrity over time, the performance of tamper detection under different attack intensities, the success rate of consistency verification, and the capability of data recovery under failures. The tampering detection rate refers to the proportion of altered data correctly identified during simulated attacks, reflecting security robustness. The results are shown in Fig. 10.

Fig. 10(a) shows that data integrity decreases most noticeably during the processing stage, dropping to about 89.5 percent. Fig. 10(b) indicates that at attack intensity level 1, the tampering detection rate of the improved PBFT is 100 percent, higher than traditional PBFT at about 98 percent and the standard blockchain at 97 percent. Even at an intensity level of 10, with 50 percent malicious nodes and ten times the baseline amount of traffic, the improved PBFT maintains a detection rate of around 94 percent. Meanwhile, traditional PBFT and the standard blockchain fall to 79 and 70 percent, respectively. Fig. 10(c) shows that system resource usage increases over time. Eventually, CPU, memory, network I/O, and storage utilization reach approximately 75, 85, 92, and close to 100 percent of their respective capacities.

To further verify the robustness and defensive capabilities of the improved PBFT algorithm in adversarial environments, a joint Sybil and DDoS attack simulation experiment is conducted. The attack scenario is implemented by injecting disguised nodes into the consensus network and applying additional traffic pressure. The attack intensity is divided into 10 levels, corresponding to malicious node ratios ranging from 5% to 50% and traffic multipliers from 1× to 10×. The system's tampering detection rate and availability are evaluated under different threat conditions by gradually increasing the attack intensity. The results are shown in Table 1.

As shown in Table 1, the detection rate and availability of the improved PBFT algorithm decreased slightly with the increase in malicious node ratio and DDoS traffic but remained at a high level overall. At attack intensity level 10, the detection rate still reaches 94.1%, and availability is maintained at 96.1%, indicating strong system stability and defense capability under high attack pressure. This is attributed to the hierarchical management of nodes and the multi-criteria scoring mechanism. These features enable the rapid identification of disguised nodes and trigger the replacement of primary nodes during attacks. This prevents consensus interruption and enhances the system's robustness in hostile environments. The collaborative efficiency test results for multiple participating entities are shown in Fig. 11.

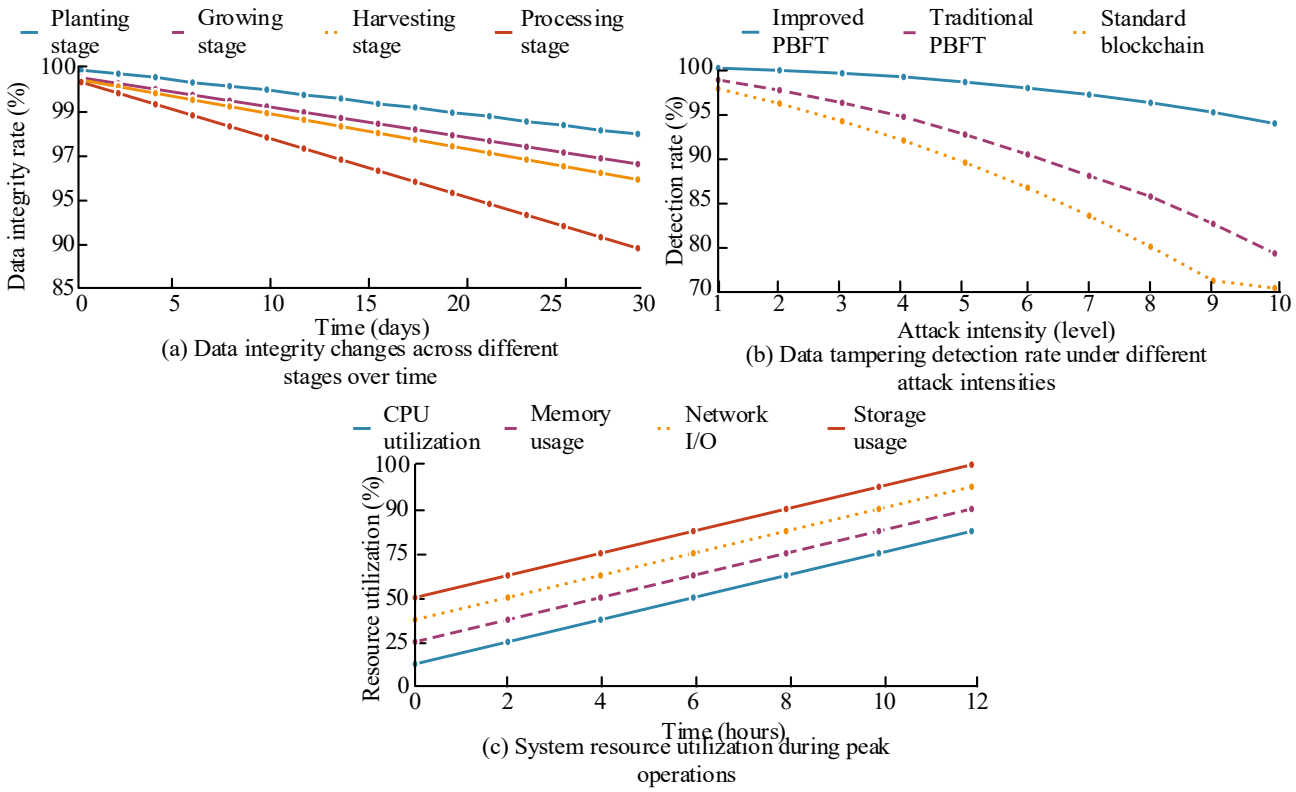

Fig. 10. Verification of integrity of traceability data for the entire life cycle of green agricultural products

Table 1. Security performance of the improved PBFT algorithm under different attack intensity levels

Attack intensity level	Malicious node ratio	DDoS traffic multiplier	Detection rate (%)	Availability (%)
1	5%	1×	99.8	99.6
2	10%	2×	99.5	99.1
3	15%	3×	98.8	98.5
4	20%	4×	98.0	97.8
5	25%	5×	97.5	97.2
6	30%	6×	96.8	96.3
7	35%	7×	96.0	95.6
8	40%	8×	95.4	90.5
9	45%	9×	94.8	94.4
10	50%	10×	94.1	96.1

As shown in Fig. 11, collaboration efficiency among multiple stakeholders is assessed quantitatively using four indicators: interaction latency, the rate at which multi-party tasks are completed, the level of participant activity, and the frequency of trust-driven collaboration. Fig. 11(a) shows that the improved PBFT significantly reduces cross-entity communication delay. The average response time to farmers is approximately 40ms, compared with more than 70ms for traditional PBFT and 150ms for a standard blockchain system. In regulator-oriented interactions, the improved PBFT maintains an average latency of about 80ms, indicating faster coordination across administrative entities. Fig. 11(b) shows that collaboration efficiency is higher. More than 90 percent of simple, two-party tasks are completed, and 45 percent of complex tasks involving six participants are completed. Fig. 11(c) indicates that participant activity remains consistently higher under the proposed system. During peak hours, the activity levels of farmers, processors, and retailers are above 85. Off-peak activity remains between 20 and 55. This suggests an improved willingness to participate in coordinated operations. Fig. 11(d) confirms that trust enhances collaboration. When the trust level is between 0.6 and 0.8, the number of medium to high frequency collaborations exceeds 70, and collaboration becomes even more intensive when the trust level is between 0.8 and 1.0. These quantitative results illustrate how blockchain strengthens coordination. The shared ledger provides unified, tamper-resistant information, reducing verification overhead. The improved PBFT accelerates cross-entity communication. The transparent trust model encourages more frequent cooperation among farmers, logistics

firms, regulators, and consumers. Overall, the system significantly enhances multi-party collaboration efficiency in real agricultural supply chain scenarios. System performance and scalability analysis are presented in Fig. 12.

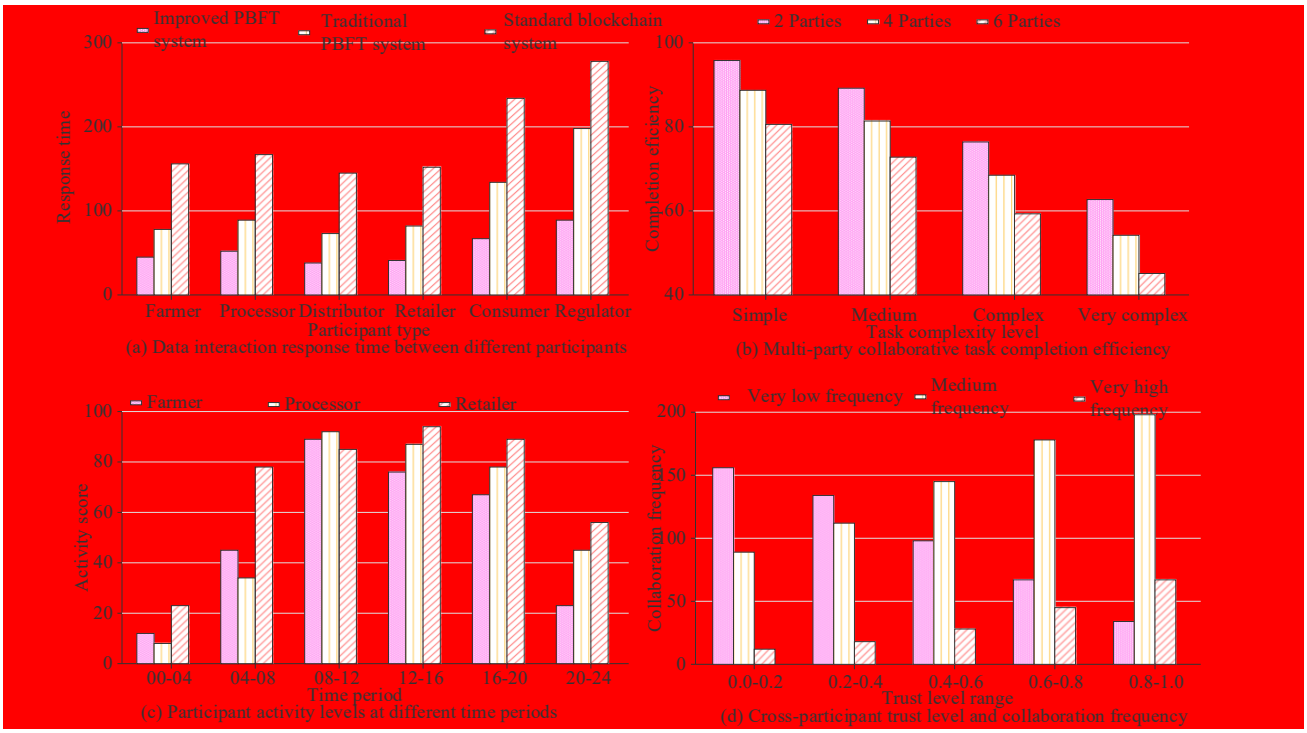

Fig. 11. Collaborative efficiency test of multiple participating entities

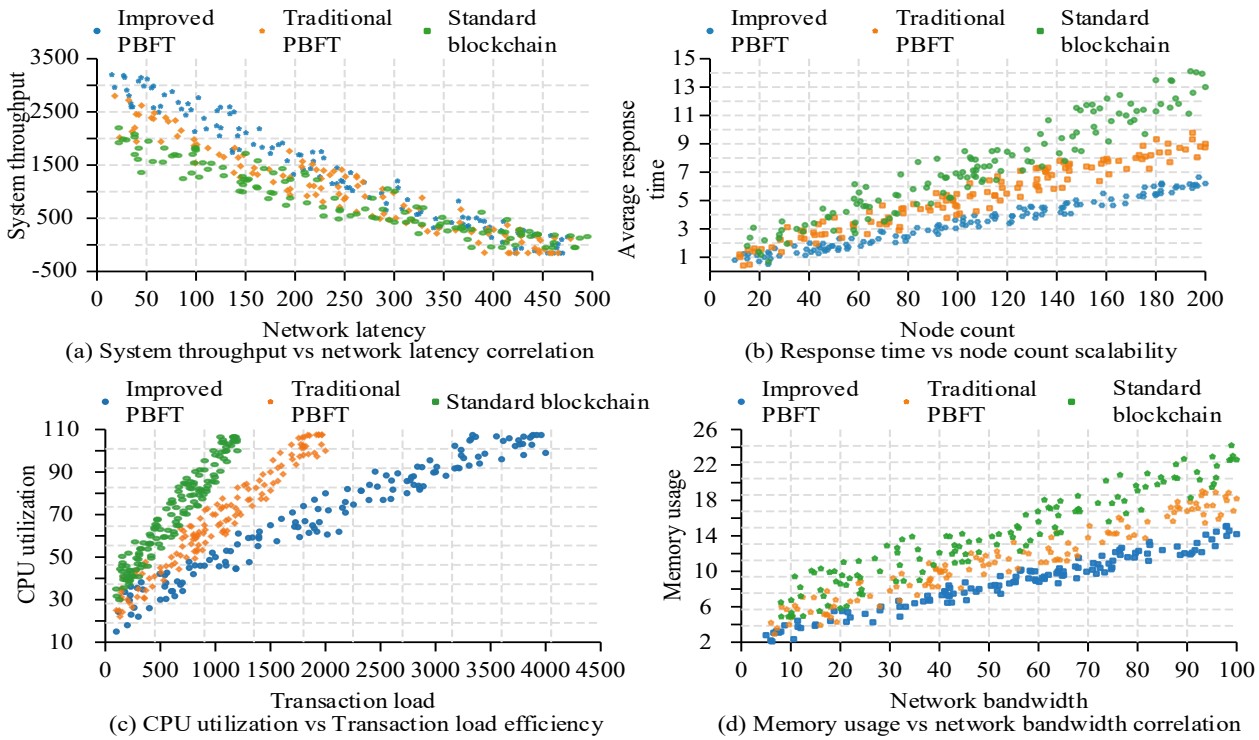

Fig. 12. System performance and scalability analysis

Fig. 12(a) shows that the improved PBFT reaches 3000 TPS at zero latency, higher than traditional PBFT at about 2500 TPS and standard blockchain at 2000 TPS. Even at 400ms latency, throughput remains above 500 TPS. Fig. 12(b) indicates that at 200 nodes, the improved PBFT records a response time of about 5ms, while traditional PBFT exceeds 8ms and standard blockchain reaches 12ms. Fig. 12(c) shows that at 500 TPS, CPU utilization is about 30 percent, lower than

traditional and standard approaches, and remains below 100 percent even at 4000 TPS. Fig. 12(d) shows that at 10 Mbps network bandwidth, memory usage is about 4 MB, compared with 6 MB and 8 MB for the other systems, and remains lower across bandwidth increases. Overall, the improved PBFT demonstrates superior performance and scalability.

To evaluate applicability in real-world deployment, a pilot is carried out in a regional tea supply chain involving 16 consortium nodes, including plantations, processing plants, warehouses, logistics providers, retailers, and a regulatory authority. The system runs continuously for four weeks, covering the entire lifecycle from harvesting to retail. It generates approximately 52,000 traceability records per day, reaching a peak load of 120 TPS. An A/B test was performed using identical data replay to compare the improved PBFT with the traditional version, focusing on system availability and traceability performance. The results are shown in Table 2.

Table 2. Key results of the tea industry pilot

Metric	Improved PBFT	Traditional PBFT
Consensus confirmation time (s)	0.21	0.33
End-to-end traceability query latency (s)	0.92	1.84
Data integrity (on-chain field completeness) (%)	98.7	96.9
Tampering detection rate (%)	98.1	95.0
System availability (%)	99.2	97.8
Peak throughput (TPS)	3300	2100

As shown in Table 2, the improved PBFT algorithm significantly reduced consensus confirmation time and end-to-end traceability latency under real business flows compared with the traditional PBFT algorithm. Data integrity and tampering detection rates improve by approximately 1.8 and 3.1 percentage points, respectively, while availability increases to 99.2%. Peak throughput reaches around 3,300 TPS, about 57% higher than the traditional implementation. These results demonstrate that, in real-world "multi-actor, multi-stage, continuous on-chain" application scenarios, the hierarchical node management combined with the multi-criteria scoring mechanism can effectively eliminate low-credibility or abnormal nodes and stably perform primary node replacement. This enhances traceability, timeliness, and trustworthiness without incurring additional business modification costs. It demonstrates strong practical deployment potential.

5. Conclusion

The improved PBFT-based blockchain traceability method effectively addressed high concurrency, heterogeneous data, and multi-party collaboration in green agricultural product traceability systems. The algorithm used hierarchical node management and a multi-indicator scoring mechanism to enable dynamic node evaluation, primary node selection, and malicious node removal. This reduced communication overhead, enhancing robustness. Experimental results showed a 50-80% increase in throughput compared with traditional algorithms, a reduction in confirmation time by about 30%, and system availability maintained above 95% under high Byzantine node ratios. In application scenarios, the method ensured data integrity and reliable traceability throughout production, processing, logistics, and sales. Even under the highest level of attacks, the tamper detection rate remained above 94%. Multi-party collaboration efficiency and trust levels were also significantly improved, which confirmed the practicality and scalability of the proposed approach.

Compared with existing improved PBFT variants, the innovation of this study lies in two key aspects. Unlike PBFT and RBFT, which optimize communication, and HotStuff and SBFT, which use more complex voting structures, the proposed "node hierarchical management+multi-index leader selection" mechanism introduces a validator set that dynamically self-optimizes and is tailored to multi-stakeholder agricultural supply chains. This mechanism enables the continuous identification and replacement of abnormal nodes, a capability largely absent in current schemes. Second, the model links node credibility with actual business processes (production, processing, logistics, etc.) and provides quantifiable collaboration metrics such as response latency and task completion rate. Experimental results confirm significant improvements in multi-party coordination. These features constitute the practical and theoretical contributions distinguishing this work from existing PBFT-based approaches.

Current work focuses on improving consensus efficiency and data reliability, and privacy protection mechanisms are not yet deeply integrated. Since traceability data may involve personal or commercially sensitive information, subsequent research will consider incorporating privacy-enhancing technologies. These technologies include differential privacy, homomorphic encryption, and zero-knowledge proofs. They would support secure and compliant data sharing. In addition, the existing node hierarchy lacks observation nodes suitable for edge computing, and the scoring mechanism's weight settings are static and cannot capture temporal behavior changes. At the application level, evaluations are conducted in a prototype environment. These evaluations do not compare to commercial traceability platforms or include green sustainability features, such as carbon footprint tracking. Future developments will include the introduction of observation nodes, the application of adaptive weighting strategies, the construction of cross-system comparison environments, and the integration of carbon emission monitoring modules. These enhancements will further improve the traceability of green agricultural products on the blockchain.

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

Declaration of Artificial Intelligence (AI) Tools

The author used ChatGPT solely for language editing and readability improvement. The author has reviewed and verified all content and takes full responsibility for the accuracy and integrity of the manuscript.

References

Chen, X., and Li, X. (2025). TinyThunder: Enabling asynchronous Byzantine fault tolerance with optimal communication efficiency. *The Computer Journal,* 68(4), 407-418. https://doi.org/10.1093/comjnl/bxae120

El Mane, A., Tatane, K., and Chihab, Y. (2024). Transforming agricultural supply chains: Leveraging blockchain-enabled Java smart contracts and IoT integration. *ICT Express,* 10(3), 650-672. https://doi.org/10.1016/j.icte.2024.03.007

Guo, X., Zhang, Y., Yao, J., and Teng, G. (2025). Performance optimization of agricultural traceability blockchain based on sharding technology. *Quality Assurance and Safety of Crops & Foods,* 17(2), 213-231. https://doi.org/10.15586/qas.v17i2.1542

Han, Y., and Fang, X. (2024). Systematic review of adopting blockchain in supply chain management: Bibliometric analysis and theme discussion. *International Journal of Production Research,* 62(3), 991-1016. https://doi.org/10.1080/00207543.2023.2236241

Huang, B., Dai, J., and Lim, J., J. (2025). Blockchain technology as a driver for sustainability? A consumer purchase intention perspective. *International Journal of Operations & Production Management,* 45(7), 1402-1425. https://doi.org/10.1108/IJOPM-04-2024-0340

Jannes, K., Beni, E., H., Lagaisse, B., and Joosen, W. (2023). BeauForT: Robust Byzantine fault tolerance for client-centric mobile web applications. IEEE Transactions on Parallel and Distributed Systems, 34(4), 1241-1252. https://doi.org/10.1109/TPDS.2023.3241963

Lai, X., Zhang, Y., and Luo, H. (2024). A low-cost blockchain node deployment algorithm for the Internet of Things. *Peer-to-Peer Networking and Applications,* 17(2), 756-766. https://doi.org/10.1007/s12083-023-01615-5

Li, C., Qiu, W., Li, X., Liu, C., and Zheng, Z. (2024). A dynamic adaptive framework for practical Byzantine fault tolerance consensus protocol in the Internet of Things. *IEEE Transactions on Computers,* 73(7), 1669-1682. https://doi.org/10.1109/TC.2024.3377921

Liu, P., Cui, X., and Li, Y. (2023). Subsidy policies of a fresh supply chain considering the inputs of blockchain traceability service system. *Science and Public Policy,* 50(1), 72-86. https://doi.org/10.1093/scipol/scac044

Mohan, V., Dhinakaran, V., Gangadharan, M., Modekurti, A., M., S., and M., J. (2023). Multi-stage energy-risk adjustments using practical Byzantine fault tolerance consensus for blockchain-powered peer-to-peer transactive markets. *Energy Conversion and Economics,* 4(4), 252-266. https://doi.org/10.1049/enc2.12092

Nayal, K., Raut, R., D., Narkhede, B., E., Priyadarshinee, P., Panchal, G., B., and Gedam, V., V. (2023). Antecedents for blockchain technology-enabled sustainable agriculture supply chain. *Annals of Operations Research*, 327(1), 293-337. https://doi.org/10.1007/s10479-021-04423-3

Okegbile, S., D., Cai, J., Chen, J., and Yi, C. (2024). A reputation-enhanced shard-based Byzantine fault-tolerant scheme for secure data sharing in zero trust human digital twin systems. *IEEE Internet of Things Journal,* 11(12), 22726-22741. https://doi.org/10.1109/JIOT.2024.3382829

Samanta, S., and Sarkar, A. (2025). Blockchain integrated DFL model for IIoT data security in smart cities. *International Journal of Information Technology,* 17(2), 911-923. https://doi.org/10.1007/s41870-024-02354-3

Somasekhar, G., Jinka, S., Kanekal, C., K., and Marouthu, A. (2024). Digital voting with blockchain using interplanetary file system and practical Byzantine fault tolerance. Engineering, *Technology & Applied Science Research,* 14(6), 19009-19015. https://doi.org/10.48084/etasr.8440

Wang, Z., F., Ren, Y., W., Cao, Z., Y., and Zhang, L., Y. (2023). LRBFT: Improvement of practical Byzantine fault tolerance consensus protocol for blockchains based on Lagrange interpolation. *Peer-to-Peer Networking and Applications,* 16(2), 690-708. https://doi.org/10.1007/s12083-022-01431-3

Xinting, Y., Rui, L., I., Jinhui, L., I., Tao, M., I., N., and Chuanheng, S., U., N. (2024). Research progress on agricultural food traceability based on blockchain technology. *Food Science,* 45(20), 299-310. https://doi.org/10.7506/spkx1002-6630-20231108-060

Yadav, V., S., Singh, A., R., Raut, R., D., and Cheikhrouhou, N. (2023). Blockchain drivers to achieve sustainable food security in the Indian context. *Annals of Operations Research,* 327(1), 211-249. https://doi.org/10.1007/s10479-021-04308-5

Zheng, J., and Zhang, Y. (2024). RSHS: A blockchain consensus mechanism for edge computing-supported Agri-IoT systems. *IEEE Transactions on Network and Service Management,* 21(4), 4104-4118. https://doi.org/10.1109/TNSM.2024.3415610

Qiaoling Yan received her Master of Finance degree from Henan University of Economics and Law in 2017. She is currently Lecturer and Director of the FinTech Section, School of Finance, Zhengzhou College of Finance and Economics. She is mainly responsible for FinTech talent cultivation. Her main research interests are FinTech, industrial economics, regional industrial chain and supply chaindigitalization, blockchain application and intelligent risk control.